REMARKS

Claims 11, 13, 14, 16-19, and 22-28 are pending. The Examiner's reconsideration of the rejection in view of the amendments and remarks is respectfully requested.

Claims 11, 13, 14, 16, 18 and 22-26 have been rejected under 35 U.S.C. 102(b) as being unpatentable over Sudia et al. (USPAN 2001/0050990). The Examiner stated essentially that Sudia teaches all of the limitations of Claims 11, 13, 14, 16, 18 and 22-26.

Claims 11, 22 and 23 are the independent claims.

Claims 11 and 22 claim, *inter alia*, executing "said signed authorized boot code having a verified digital signature by branching to a copy of said signed authorized boot code in said protected memory, said signed authorized boot code including instructions for performing a boot process for a computer device comprising the processor." Claim 23 claims, *inter alia*, "a processor comprising includes inline cryptography and integrity hardware for executing boot code in signal communication with said protected memory executing said signed authorized code from the protected memory for booting the computing device after verifying that a digital signature contained in said signed authorized code is original in accordance with a first public key stored in said protected memory." Claims 11, 22 and 23 have been clarified to specify that the signed authorized code is executed by the processor and that the code embodies a boot process (see for example, paragraphs [0022-0024] of the published application).

Sudia teaches a cryptographic system with a key escrow feature (see Abstract). Sudia does not teach executing "said signed authorized boot code having a verified digital signature by branching to a copy of said signed authorized boot code in said protected memory" as claimed in Claims 11 and 22 or "a processor comprising inline cryptography and integrity hardware for

executing boot code" as claimed in Claim 23.

Sudia teaches how to perform a desired upgrade instructions in a tamper-resistance trusted device (see paragraph [0250]). The upgrade process presumes that the trusted device is booted. Sudia does not consider how to perform the upgrade process, much less execute the upgrade firmware, at boot time. For example, Sudia fails to teach that a processor includes inline cryptography and integrity hardware for executing boot code, essentially as claimed in Claim 23. Consider that Sudia teaches that the "basic cryptographic library routines" are stored in firmware (see paragraphs [0097-0099]). Sudia makes use of cryptography software or code without the ability to perform such operations prior to booting the trusted device.

Claims 13, 14, 16-19 depend from Claim 11. The dependent claims are believed to be allowable for at least the reasons given for Claim 11. Claims 15, 20 and 21 have been cancelled. The Examiner's reconsideration of the rejection is respectfully requested.

Claims 17, 19, 27 and 28 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia in view of Morgan et al. (USPN 6,185,685). The Examiner stated essentially that the combined teachings of Sudia and Morgan teach or suggest all of the limitations of Claims 17, 19, 27 and 28.

Claims 17 and 19 depend from Claim 11. Claims 27 and 28 depend from Claim 23. The dependent claims are believed to be allowable for at least the reasons given for the respective independent claims. Reconsideration of the rejection is respectfully requested.

For the forgoing reasons, the application, including Claims 11, 13, 14, 16-19, and 22-28, is believed to be in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Respectfully submitted,

Dated: February 23, 2011

By: /Nathaniel T. Wallace/
Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Applicants

F. CHAU & ASSOCIATES, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889